ABSTRACT

The present invention is a method of creating a secure sandbox within which a plurality of downloaded software components can execute in a secure manner. The software components can be of any type, e.g., Java, ActiveX, Netscape plugin, etc. The invention implements a security monitor that is injected to the address space of an arbitrary monitored application such as a Web browser, e.g., Internet Explorer, Netscape Navigator, etc. The monitored application then executes in a secure mode in which every software component downloaded executes in a secure sandbox. The security monitor detects when such a software component is downloaded and is operative to create the sandbox around it before it is permitted to execute. If the software component attempts to commit an action that breaches security, it halts the software component's execution and issues a warning to the user. The security monitor detects attempted security breaches by the software component in accordance with a user configurable security policy. Such a policy may include limiting file read/write access, access to directories, disk access, creation and the reading/writing of network connections, access to system resources and services and access to the address spaces of other processes.

09825102 . 032702